An Elliptic Curve Implementation of the Finite Field Digital Signature Algorithm

Neal Koblitz

Dept. of Mathematics, Box 354350, Univ. of Washington
Seattle, WA 98195 U.S.A., koblitz@math.washington.edu

Abstract. We construct a supersingular implementation of the Elliptic Curve Digital Signature Algorithm (ECDSA) that is essentially equivalent to a finite field implementation of the Digital Signature Algorithm (DSA), and then we compare the efficiency of the two systems. The elliptic curve method is about 12 times faster. In the last section we use the same ideas to give a particularly efficient nonsupersingular implementation of elliptic curve cryptography in characteristic 7.

Key Words: Digital Signature, Elliptic Curve, Supersingular, Nonadjacent Form

1 Introduction

The security of elliptic curve cryptosystems depends on the presumed intractability of the discrete logarithm problem in the group of points on the curve. Aside from the exponential time algorithms that apply to an arbitrary group — all of which are impractical if the order of the group is divisible by a prime of more than 40 decimal digits — the only discrete log algorithms that have been found for an elliptic curve group are the algorithm of Semaev–Smart–Satoh–Araki [20, 22, 17], which applies only to an elliptic curve over a prime field $\mathbf{F}_p$ whose order is equal to p, and the algorithm of Menezes–Okamoto–Vanstone (MOV) [12]. The MOV algorithm uses the Weil pairing to imbed the group of points of an elliptic curve E over a finite field $\mathbf{F}_q$ into the multiplicative group $\mathbf{F}_{q^K}^\times$ of an extension field $\mathbf{F}_{q^K}$; the elliptic curve discrete log problem then reduces to the discrete log problem in $\mathbf{F}_{q^K}^\times$. This algorithm is practical if K can be taken to be small. If E is a supersingular elliptic curve, then K can always be chosen equal to 1, 2, 3, 4, or 6 [12]; whereas if E is nonsupersingular, then K is almost always much too large [1]. For this reason it is usually assumed that supersingular curves should not be used in cryptography.

The purpose of this article is to give a cryptographic application of a family of supersingular elliptic curves for which $K = 6$ in the MOV algorithm. Suppose that $\#E(\mathbf{F}_q)$ is a prime l (or a very small integer factor times a prime l) of between 40 and 80 decimal digits (which is the range one would use with a

nonsupersingular curve). Then $q^K = q^6$ is roughly in the 250- to 500-digit range, which is beyond the practical limits of algorithms for the discrete log in $\mathbf{F}_{q^K}^\times$. Thus, such a family of curves can be used in cryptography.

Moreover, the family of curves that we study lends itself to particularly efficient computation of a multiple of a point, which is the basic operation in elliptic curve cryptosystems. Because the curves have complex multiplication by cube roots of unity, this family can be treated in a manner similar to the family of anomalous binary curves that was studied in [6], [10], and [23]. §§2–3 are devoted to the properties of the curves we are proposing and to the use of a special type of ternary expansion of an integer k that allows one to compute kP with only $\approx \frac{2}{5}\log_3 q$ elliptic curve additions.

In §§4–5 we describe our main motivation for looking at this family of supersingular elliptic curves: it enables us in characteristic 3 to make a very direct comparison of efficiency between the Digital Signature Algorithm (DSA) using finite fields (see [16]) and the Elliptic Curve Digital Signature Algorithm (ECDSA) (see, for example, [9]). Recall that in DSA one works in a cyclic subgroup of prime order l inside a finite field whose bitlength is between 3 and 6 times that of l. Thus, it would be completely consistent with the Digital Signature Standard to take $\mathbf{F}_{q^6}$ as one's finite field and the image of $E(\mathbf{F}_q)$ under the MOV imbedding as one's cyclic subgroup of order l. Then, conjecturally, the ECDSA and the corresponding DSA have identical security, and so it is interesting to compare efficiency. We show that the elliptic curve implementation is about 12 times as fast. In other words, even though the two groups of order l are apparently cryptographically equivalent, the elliptic curve "exponentiation" can be carried out more rapidly than exponentiation in the finite field.

Remark. We say "conjecturally" and "apparently" because we do not know how to prove that the discrete log problem on the elliptic curve group could not be easier than the discrete log problem in the corresponding subgroup of $\mathbf{F}_{q^6}^\times$. This is because we do not know how to compute the inverse of the imbedding $E(\mathbf{F}_q) \hookrightarrow \mathbf{F}_{q^6}^\times$ given by the Weil pairing.

Finally, in §6 we use the same ideas as in §§2–3 to give a family of nonsupersingular elliptic curves in characteristic 7 for which one also has a particularly efficient method to compute multiples of points.

2 The Curves

Let $q = 3^m$, where m is not divisible by 2 or 3, and let $a = 0$ or 1. Let E be the elliptic curve

$$Y^2 = X^3 - X - (-1)^a \tag{1}$$

over the field of 3 elements $\mathbf{F}_3$; and let N_m denote the number of $\mathbf{F}_q$-points on E. Because $x^3 - x = 0$ for all $x \in \mathbf{F}_3$, it is easy to see that $N_1 = 4 - (-1)^a 3$. We can also write $N_1 = 4 - \tau - \overline{\tau}$, where

$$\tau = \frac{(-1)^a 3 + i\sqrt{3}}{2}$$

is the root with positive imaginary part of the characteristic polynomial $T^2 - (-1)^a 3T + 3$ of the Frobenius map $\Phi : (x, y) \mapsto (x^3, y^3)$.[1] In other words, τ satisfies the relation

$$3 = (-1)^a 3\tau - \tau^2. \tag{2}$$

Then, by Weil's theorem,

$$N_m = |\tau^m - 1|^2 = 3^m - (-1)^a \left(\frac{3}{m}\right) 3^{(m+1)/2} + 1, \tag{3}$$

where $\left(\frac{3}{m}\right)$ is the Jacobi symbol, which is defined as follows:

$$\left(\frac{3}{m}\right) = \begin{cases} 1 & \text{if } m \equiv \pm 1 \pmod{12}; \\ -1 & \text{if } m \equiv \pm 5 \pmod{12}. \end{cases}$$

Since N_m is divisible by $N_{m'}$ whenever $m'|m$, we have the best chance of getting a large prime factor of N_m when m is prime. In that case $N_1|N_m$, but it may happen that N_m/N_1 is prime. In other words, when m is prime N_m could be a prime in the case $a = 0$ and 7 times a prime in the case $a = 1$. For example, when $a = 0$ we find that $N_{163} = 3^{163} + 3^{82} + 1$ is a prime of 78 decimal digits (259 bits); and when $a = 1$ we find that $N_{97} = 3^{97} + 3^{49} + 1$ is 7 times a prime of 46 decimal digits (154 bits).

Remark. One might want to use composite m in order to be able to perform multiplications and inversions in $\mathbf{F}_{3^m}$ more efficiently using a tower of subfields. It is still possible to get a large prime factor of N_m with m not much larger than in the case when m is prime. For example, when $a = 0$, a 66-digit prime divides N_{169}; and when $a = 1$, a 47-digit prime divides N_{121}, and a 74-digit prime divides N_{187}.

We let ω denote the 6th root of unity

$$\omega = \tau - (-1)^a = \frac{(-1)^a + i\sqrt{3}}{2}, \tag{4}$$

and we let $\mathbf{Z}[\omega]$ denote the ring of integers of the form $u + v\omega$, $u, v \in \mathbf{Z}$. Then when m is prime we are interested in primality of the element $(\omega+1)^m - 1$ when $a = 0$ and primality of the element $((\omega - 1)^m - 1)/(\omega - 2)$ when $a = 1$, since it is a prime element of $\mathbf{Z}[\omega]$ if and only if

$$\frac{N_m}{N_1} = \begin{cases} |(\omega + 1)^m - 1|^2, & \text{if } a = 0; \\ \frac{1}{7}|(\omega - 1)^m - 1|^2, & \text{if } a = 1, \end{cases}$$

is a prime in $\mathbf{Z}$. When $a = 0$ this is a close analogue of the Mersenne prime problem, as we see by replacing ω by 1. (This example of an elliptic curve

[1] This means that $\left(\Phi^2 - (-1)^a 3\Phi + 3\right) P = O$ for any point P on the curve. This polynomial (more precisely, its reciprocal polynomial $1 - (-1)^a 3T + 3T^2$) is also the numerator of the zeta-function of the curve. For details on this and other properties of elliptic curves, see §VI.1 of [7] and Ch. V of [21].

for cryptography and the analogy with the Mersenne prime problem were first mentioned in Exercise 11 of §VI.1 and Exercise 6 of §VI.2 in [7].)

As always, the Frobenius map $\Phi : (x, y) \mapsto (x^3, y^3)$ takes negligible time, provided that we are working in a normal basis of $\mathbf{F}_q$ over $\mathbf{F}_3$; and the negation map $(x, y) \mapsto (x, -y)$ is also trivial to carry out. The Frobenius map Φ acting on points $P \in E(\mathbf{F}_q)$ may be regarded as the element $\tau \in \mathbf{Z}[\omega]$, because it satisfies the same quadratic equation $\Phi^2 - (-1)^a 3\Phi + 3 = 0$.

In the case of the particular equation (1), it is also extremely easy to describe the action on points $P \in E(\mathbf{F}_q)$ of the cube roots of unity. Let us take $a = 1$; the case $a = 0$ is virtually identical. Then we are interested in how the nontrivial cube root of unity $\omega = (-1 + \sqrt{3}i)/2 = \tau + 1$ acts on $P = (x, y) \in E(\mathbf{F}_q)$. That is, we want to find the coordinates of $(\Phi + 1)P = P_{x,y} + P_{x^3,y^3}$. Using the addition law for $P_{x_1,y_1} + P_{x_2,y_2} = P_{x_3,y_3}$, which takes the following form when $P_{x_2,y_2} \neq \pm P_{x_1,y_1}$:

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2;$$
$$y_3 = y_1 + y_2 - \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^3,$$

and the relation $x^3 - x = y^2 - 1$ from (1), we obtain:

$$P_{x,y} + P_{x^3,y^3} = P_{x+1,y}.$$

(It is easy to check that this formula also holds when $P_{x^3,y^3} = P_{x,y}$, i.e., when $P_{x,y}$ is an $\mathbf{F}_3$-point.) Thus, the action on points of any power of τ and any sixth root of unity can be computed in trivial time.

Remark. Another convenient feature of the curves (1) in characteristic 3 is that, if we use a normal $\mathbf{F}_3$-basis $\{\beta, \beta^3, \ldots, \beta^{3^{m-1}}\}$ of $\mathbf{F}_q$, then there is an easy compression technique for storing a point $P_{x,y}$, by analogy with the characteristic 2 method in [13]. Namely, we represent P as (x_0, y), where $x_0 \in \{0, 1, -1\}$ is the first coordinate of x. Then $x = \sum x_i \beta^{3^i}$ can be recovered by setting $x_i = x_{i-1} + z_i$, $i = 1, 2, \ldots, m-1$, where the z_i are the coordinates of $-y^2 - (-1)^a = \sum z_i \beta^{3^i}$.

3 Base-τ Expansions

Suppose that we want to compute a multiple kP of an $\mathbf{F}_{3^m}$-point on the elliptic curve (1). As in [10] and [23], our first step is to divide k by $\tau^m - 1$ in the ring $\mathbf{Z}[\omega]$, and then replace k by its remainder k' modulo $\tau^m - 1$. This is justified because $(\tau^m - 1)P = \Phi^m P - P = O$. Our next step is to find a base-τ expansion of k' with digits $\{0, \pm 1, \pm\omega, \pm\omega^2\}$ that has *nonadjacent form* (NAF), where, following [23], we define "nonadjacent form" to mean that no two consecutive coefficients are nonzero.

Theorem 1 *Every element of* $\mathbf{Z}[\omega]$ *reduced modulo* $\tau^m - 1$ *has a unique NAF base-*τ *expansion with digits* $\{0, \pm 1, \pm\omega, \pm\omega^2\}$, *in which at most* $(m+1)/2$ *digits are nonzero. Asymptotically on the average 60% of the digits are zero.*

Proof. We first recall the algorithm for finding the usual base-τ expansion of an element $u + v\omega \in \mathbf{Z}[\omega]$ with digits $\epsilon_j \in \{0, 1, -1\}$. By (4) we have $u + v\omega = (u - (-1)^a v) + v\tau$. Dividing the integer $u - (-1)^a v$ by 3, we can write $u - (-1)^a v = 3w + \varepsilon_0$ for some $\varepsilon_0 \in \{0, 1, -1\}$. Then we use (2) to write $u + v\omega = (3w + \varepsilon_0) + v\tau = (((-1)^a 3w + v) - w\tau)\,\tau + \varepsilon_0$. We then take the quotient $((-1)^a 3w + v) - w\tau$ and repeat the process to find ε_1, ε_2, and so on.

Now we describe the algorithm for finding the NAF base-τ expansion of an element of $\mathbf{Z}[\omega]$. In each step we divide our previous quotient q_{j-1} by τ, getting a quotient $u + v\tau$ and a remainder $\varepsilon \in \{0, 1, -1\}$, as we did in the previous paragraph:

$$q_{j-1} = (u + v\tau)\tau + \varepsilon.$$

If $\varepsilon = 0$ or if $3|u$, then we leave the above equality unchanged and set $q_j = u + v\tau$, $\eta_j = \varepsilon$. Otherwise, we modify the above equation as follows:

$$q_{j-1} = q_j\tau + \eta_j,$$

where

$$q_j = \begin{cases} (u + (-1)^a 2\varepsilon) + (v - \varepsilon)\tau & \text{if } u \equiv (-1)^a \varepsilon \pmod 3; \\ (u + (-1)^a \varepsilon) + v\tau & \text{if } u \equiv -(-1)^a \varepsilon \pmod 3, \end{cases}$$

and

$$\eta_j = \begin{cases} -(-1)^a \varepsilon \overline{\omega} & \text{if } u \equiv (-1)^a \varepsilon \pmod 3; \\ -(-1)^a \varepsilon \omega & \text{if } u \equiv -(-1)^a \varepsilon \pmod 3. \end{cases}$$

Uniqueness of the NAF expansion is clear from the construction. Finally, the asymptotic expectation is that every nonzero digit is followed by $1 + \frac{1}{3} + \frac{1}{3^2} + \cdots = 1.5$ zero digits, in which case 60% of the digits are zero. □

Here is an example. Let us take $a = 0$ and find the expansion of $10 + 2i\sqrt{3}$. We have:

$$\begin{aligned} 10 + 2i\sqrt{3} &= (7 - \tau)\tau + 1 \\ &= (9 - 2\tau)\tau + \omega^2; \\ 9 - 2\tau &= (7 - 3\tau)\tau + 0; \\ 7 - 3\tau &= (3 - 2\tau)\tau + 1; \\ 3 - 2\tau &= (1 - \tau)\tau + 0; \\ 1 - \tau &= 0 \cdot \tau + \omega^4, \end{aligned}$$

and hence the digits are $\eta_4 = \omega^4$, $\eta_3 = 0$, $\eta_2 = 1$, $\eta_1 = 0$, $\eta_0 = \omega^2$.

Remark. The expected number $\frac{2}{5}\log_3 q$ of elliptic curve additions given by Theorem 1 is about 25% less than the previous lowest result for the number of additions of points in computing kP, which was $\frac{1}{3}\log_2 q$ due to Solinas [23]. However, from a practical point of view this improvement in the number of elliptic curve additions might be offset by the decreased efficiency of working in characteristic 3 rather than 2. For example, in characteristic 2 one can often minimize time for a field operation by using an optimal normal basis [15].

In order to avoid field inversions and determine the time required to compute a multiple of a point in terms of field multiplications alone, we introduce projective coordinates. (See §6.3 of [11] for a discussion of this in characteristic 2.) When converted to homogeneous coordinates, the equations for point addition (see §2) become

$$\begin{aligned} z_3 &= (x_2z_1 - x_1z_2)^3 z_1 z_2; \\ x_3 &= (y_2z_1 - y_1z_2)^2(x_2z_1 - x_1z_2)z_1z_2 - (x_2z_1 - x_1z_2)^3 x_1z_2 - \\ &\quad -(x_2z_1 - x_1z_2)^3 x_2z_1; \\ y_3 &= -(x_2z_1 - x_1z_2)^3 y_1z_2 + (y_2z_1 - y_1z_2)(x_2z_1 - x_1z_2)^2 x_1z_2 - \\ &\quad -x_3(y_2z_1 - y_1z_2)/(x_2z_1 - x_1z_2). \end{aligned}$$

(Note that the last expression is a polynomial, because x_3 is divisible by $x_2z_1 - x_1z_2$.)

In each stage of the computation of kP one adds a partial sum to a point of the form $\eta_j \tau^j P$ (in which the NAF digit η_j is a sixth root of unity). The latter point is computed in negligible time in affine (i.e., non-homogeneous) coordinates; so we may assume that its projective coordinates are $(x_2, y_2, 1)$, that is, $z_2 = 1$. Assuming now that $z_2 = 1$, the above formulas can be computed as follows. Successively set

$$A = x_2z_1; \qquad B = y_2z_1; \qquad C = (A - x_1)^2; \qquad D = (A - x_1)^3;$$

$$E = (B - y_1)^2; \qquad F = x_1C; \qquad G = z_1E - (D + 2F).$$

Then

$$z_3 = z_1D; \qquad x_3 = (A - x_1)G; \qquad y_3 = -y_1D + (B - y_1)(F - G).$$

This all takes 10 field multiplications. (Note that D is computed in negligible time, since we are in characteristic 3.)

Since on the average $\frac{2}{5}m$ point additions are needed to compute a multiple of a point, it follows that in projective coordinates one expects to compute a multiple of a point with $4m$ field multiplications.

From the formulas for adding points in affine coordinates (see §2) we see that, alternatively, a point addition can be accomplished with 1 field inversion and 2 field multiplications. Thus, if an inversion can be done in less time than 8 field multiplications, we should use affine rather than projective coordinates. In characteristic 2 there are implementations of field inversion that take time roughly equal to that of 3 field multiplications (see [19] and [24]); and it is reasonable to expect that the same equivalence can be achieved in characteristic 3 [18].

We have obtained the following corollary of Theorem 1.

Corollary 1 *If one uses projective coordinates, the expected number of field multiplications in* $\mathbf{F}_{3^m}$ *needed to compute a multiple of a point on the curve (1) is* $4m$. *Using affine coordinates, on the average one can compute a multiple of a*

point on (1) with $\frac{4}{5}m$ field multiplications and $\frac{2}{5}m$ field inversions. If a field inversion can be carried out in time equivalent to that of three field multiplications, then in affine coordinates one has a time estimate of $2m$ field multiplications for computing a multiple of a point.

4 DSA and ECDSA

We shall use DSA in a slightly generalized form, in which the finite field $\mathbf{F}_q$, $q = p^m$, is not necessarily a prime field. Here q has at least 500 bits, and $q-1$ is divisible by a prime l of at least 160 bits. Let $f : \mathbf{F}_q \to \mathbf{F}_l$ be a fixed, easily computable function such that $\#f^{-1}(y) \approx q/l$ for each $y \in \mathbf{F}_l$; that is, f spreads $\mathbf{F}_q$ fairly evenly over $\mathbf{F}_l$. If $q = p$, then we represent elements of $\mathbf{F}_q$ by integers $x \in \{0, 1, \ldots, p-1\}$, and we usually take $f(x)$ to be the least nonnegative residue of x modulo l. If $m > 1$, and if $\{\beta_0, \ldots, \beta_{m-1}\}$ is our $\mathbf{F}_p$-basis of $\mathbf{F}_q$, then for $x = \sum x_i\beta_i$, $x_i \in \{0, 1, \ldots, p-1\}$, we could, for example, define $f(x)$ to be the least nonnegative residue modulo l of the integer $\sum x_i p^i$.

Let $g \in \mathbf{F}_q$ be a generator of the unique subgroup of $\mathbf{F}_q^\times$ of order l, and let H be a hash function taking values in $\mathbf{F}_l$. Here q, l, $\{\beta_i\}$, g, f, and H are publicly known. Alice's secret key is a random integer x in the range $1 < x < l$, and her public key is $y = g^x \in \mathbf{F}_q$.

To sign a message M, Alice does the following:
1) She selects a random integer k in the range $1 < k < l$.
2) She computes $g^k \in \mathbf{F}_q$ and $r = f(g^k)$. If $r = 0$, she returns to step 1).
3) She computes $k^{-1} \in \mathbf{F}_l$ and $s = k^{-1}(H(M) + xr) \in \mathbf{F}_l$. If $s = 0$, she returns to step 1).
4) Her signature for the message M is the pair (r, s).

To verify the signature, Bob computes $u_1 = s^{-1}H(M) \in \mathbf{F}_l$, $u_2 = s^{-1}r \in \mathbf{F}_l$, and then $g^{u_1}y^{u_2} \in \mathbf{F}_q$. If $f(g^{u_1}y^{u_2}) = r$, he accepts the signature.

We now describe the elliptic curve version ECDSA. Let E be an elliptic curve defined over $\mathbf{F}_q$ such that $\#E(\mathbf{F}_q)$ is equal to a prime l of at least 160 bits (or to a small integer factor times such a prime l). Let P be an $\mathbf{F}_q$-point of E of order l. Let $f_E : E(\mathbf{F}_q) \to \mathbf{F}_l$ be a fixed, easily computable function that spreads the points over $\mathbf{F}_l$ fairly evenly (for instance, we might require that $\#f_E^{-1}(y)$ be bounded by a small constant for $y \in \mathbf{F}_l$). One way to define the elliptic curve function f_E, for example, would be to take the x-coordinate of a point and then apply to it the function $f : \mathbf{F}_q \to \mathbf{F}_l$ in the above description of DSA.

Alice's secret key is an integer x in the range $1 < x < l$, and her public key is the point $Q = xP \in E(\mathbf{F}_q)$. To sign a message M, Alice does the following:
1) She selects a random integer k in the range $1 < k < l$.
2) She computes kP and $r = f_E(kP)$. If $r = 0$, she returns to step 1).
3) She computes $k^{-1} \in \mathbf{F}_l$ and $s = k^{-1}(H(M) + xr) \in \mathbf{F}_l$. If $s = 0$, she returns to step 1).
4) Her signature for the message M is the pair (r, s).

To verify the signature, Bob computes $u_1 = s^{-1}H(M) \in \mathbf{F}_l$, $u_2 = s^{-1}r \in \mathbf{F}_l$, and then $u_1P + u_2Q \in E(\mathbf{F}_q)$. If $f_E(u_1P + u_2Q) = r$, he accepts the signature.

5 Comparison of DSA and ECDSA

We set up ECDSA using the curve E in (1) over $\mathbf{F}_q$, $q = 3^m$. We assume that

$$l = \frac{N_m}{N_1} = \left|\frac{\tau^m - 1}{\tau - 1}\right|^2 = \begin{cases} 3^m - \left(\frac{3}{m}\right) 3^{(m+1)/2} + 1, & \text{if } a = 0; \\ \left(3^m + \left(\frac{3}{m}\right) 3^{(m+1)/2} + 1\right)/7, & \text{if } a = 1, \end{cases}$$

is prime. Let $P \in E(\mathbf{F}_q)$ be a point of order l.

Let $F : E(\mathbf{F}_q) \to \mathbf{F}_{q^6}^\times$ be an MOV imbedding of the elliptic curve group into the multiplicative group of $\mathbf{F}_{q^6}$ constructed using the Weil pairing [12]. Let $g = F(P)$, which is a generator of the unique subgroup of $\mathbf{F}_{q^6}^\times$ of order l.

We set up DSA in $\mathbf{F}_{q^6}^\times$ and ECDSA in $E(\mathbf{F}_q)$ so as to be equivalent to one another by means of F. Thus, if $f : \mathbf{F}_{q^6} \to \mathbf{F}_l$ is the function in DSA, then we define $f_E : E(\mathbf{F}_q) \to \mathbf{F}_l$ by the formula $f_E = f \circ F$.

Remark. In a practical situation it would be more efficient to define f_E without using the MOV imbedding F (for example, by applying f to the x-coordinate of a point, as suggested in §4), because even though the computation of F is polynomial time, it is not very fast. We have chosen to set $f_E = f \circ F$ for a theoretical rather than practical reason: to make the DSA and ECDSA implementations completely equivalent.

We can now easily verify that the MOV imbedding F gives an equivalence between the two signature schemes. In both cases Alice's secret key is an integer x in the range $1 < x < l$; her public key is $Q = xP$ in ECDSA and $F(Q) = F(xP) = F(P)^x = g^x = y$ in DSA. The k, r, and s are the same in both cases. So are the u_1 and u_2 in signature verification. In ECDSA the signature is verified by computing $u_1P + u_2Q$, and in DSA by computing $g^{u_1}y^{u_2}$. The signature is accepted if

$$\begin{aligned} r &= f_E(u_1P + u_2Q) \\ &= f(F(u_1P + u_2Q)) \\ &= f(g^{u_1}y^{u_2}). \end{aligned}$$

Thus, the DSA and ECDSA implementations are equivalent.

In order to get an approximate idea of the relative efficiency of the two systems, let us compare the times to compute 1) $kP \in E(\mathbf{F}_q)$ and 2) $g^k \in \mathbf{F}_{q^6}$, where k is a random integer in the range $1 < k < l$, i.e., k has about the same bitlength as $q = 3^m$. We shall neglect possible speed-ups using precomputations, fast multiplication techniques, etc., and shall assume that a field multiplication in $\mathbf{F}_q$ takes time proportional to $(\log_2 q)^2$.

We shall also assume that a field inversion in $\mathbf{F}_q$ takes approximately the same amount of time as 3 field multiplications; in that case the computation of kP on the average takes the equivalent of $2m$ field multiplications in $\mathbf{F}_q$, by the corollary to Theorem 1 (see §3).

On the DSA side, we have a significant efficiency advantage because we are working in characteristic 3. Namely, we first write the exponent k in ternary form as $k = \sum \varepsilon_j 3^j$, where $\varepsilon_j \in \{0, 1, 2\}$. For $\nu = 0, 1, 2$ let J_ν be the set of j for which

$\varepsilon_j = \nu$. Since the computation of g^{3^j} takes negligible time, the computation of $g^k = \prod_{j \in J_1} g^{3^j} \left(\prod_{j \in J_2} g^{3^j} \right)^2$ takes just $\#(J_1) + \#(J_2)$ field multiplications. We expect about one third of the digits in k to be zero, so we conclude that the computation of g^k takes roughly $\frac{2}{3}m$ field multiplications in $\mathbf{F}_{q^6}$, each of which takes about 36 times as long as a field multiplication in $\mathbf{F}_q$.

Thus, the ratio of time for g^k to time for kP is roughly

$$\frac{36 \cdot \frac{2}{3}m}{2m} = 12.$$

In other words, when we choose parameters for ECDSA and for DSA in such a way as to make the two systems equivalent, we find that ECDSA is approximately 12 times faster than DSA, independently of the value of m.

6 A Nonsupersingular Family

Consider the curve

$$Y^2 = X^3 - b, \qquad b \neq 0,$$

defined over $\mathbf{F}_7$. This elliptic curve is nonsupersingular. The number $N_1 = 8 - t$ of $\mathbf{F}_7$-points and the root τ with positive imaginary part of the characteristic polynomial $T^2 - tT + 7$ are given in the following table:

b	t	τ
± 1	± 4	$\pm 2 + \sqrt{3}i$
± 2	± 1	$(\pm 1 + 3\sqrt{3}i)/2$
± 3	± 5	$(\pm 5 + \sqrt{3}i)/2$

As usual, we choose b and a prime m so that $N_m/N_1 = |(\tau^m - 1)/(\tau - 1)|^2$ is prime. For instance, when $b = -1$ the number N_{59} is 12 times a 49-digit prime; and when $b = 3$ the number N_{61} is 3 times a 52-digit prime, and the number N_{71} is 3 times a 60-digit prime.

Note that, up to complex conjugation, the six value of τ in the table differ from one another by a factor of ± 1, $\pm\omega$, or $\pm\omega^2$, where $\omega = (-1 + \sqrt{3}i)/2$.

As before, we define the action of τ on a point $P \in E(\overline{\mathbf{F}}_7)$, where $\overline{\mathbf{F}}_7 = \bigcup_m \mathbf{F}_{7^m}$ is the algebraic closure of $\mathbf{F}_7$, to be the Frobenius map $\tau P_{x,y} = \Phi P_{x,y} = P_{x^7,y^7}$. In this way $\mathbf{Z}[\omega]$ imbeds in the ring of endomorphisms of $E(\overline{\mathbf{F}}_7)$; and it follows from the properties of nonsupersingular curves (see p. 137 of [21]) that the image of $\mathbf{Z}[\omega]$ is *all* of the endomorphism ring of $E(\overline{\mathbf{F}}_7)$.

It is easy to check that the maps $P_{x,y} \mapsto P_{2x,y}$ and $P_{x,y} \mapsto P_{4x,y}$ are endomorphisms of $E(\overline{\mathbf{F}}_7)$ of order 3. Since $\omega = (-1 + \sqrt{3}i)/2$ and $\omega^2 = \overline{\omega}$ are the only nontrivial cube roots of unity, it follows that in each case ωP must be given by one of these maps; one can quickly determine which of the two by testing on an $\mathbf{F}_7$- or $\mathbf{F}_{7^2}$-point of E. Thus, the action on $\mathbf{F}_{7^m}$-points of any of the sixth roots of unity ± 1, $\pm\omega$, $\pm\omega^2$ is trivial to compute.

Suppose that we want to compute a multiple kP for $P \in E(\mathbf{F}_{7^m})$. As usual, we first replace k by its remainder $k' \in \mathbf{Z}[\omega]$ after division by $\tau^m - 1$. We then compute the base-τ expansion of k' using $\{0, \pm 1, \pm\omega, \pm\omega^2\}$ rather than $\{0, \pm 1, \pm 2, \pm 3\}$ as digits; this is easy to do using the equality $\tau^2 = t\tau - 7$ and the simple relations between τ, ω, and $\pm 2, \pm 3$. We cannot obtain an NAF expansion, but we have the advantage that k' has fewer digits in characteristic 7, where the base τ has larger norm (7 rather than 2 or 3). Since 1/7 of the digits are expected to be 0, we conclude that on the average the computation of kP requires $\approx \frac{6}{7}\log_7 q = 0.3052 \log_2 q$ elliptic curve additions.

This estimate for the number of elliptic curve additions is slightly lower than Solinas' value of $\frac{1}{3}\log_2 q$ on an anomalous binary curve [23]. But in practice the improvement from $\frac{1}{3}\log_2 q$ to $0.3052 \log_2 q$ is not enough to compensate for the lower efficiency of working in characteristic 7 rather than in characteristic 2.

Remark. A disadvantage of this family of curves is that there are not many curves and fields to choose from. The same applies to the curves in §2, and to the anomalous binary curves in [6, 10, 23]. Random curves allow far more choice, but less efficient implementation.

Acknowledgments: I would like to thank Arjen Lenstra, Richard Schroeppel, and Alfred Menezes for several very helpful comments and suggestions.

References

1. R. Balasubramanian and N. Koblitz, The improbability than an elliptic curve has subexponential discrete log problem under the Menezes–Okamoto–Vanstone algorithm, *J. Cryptology* **11** (1998), 141-145.
2. I. Blake, X. H. Gao, R. C. Mullin, S. A. Vanstone, and T. Yaghoobian, *Applications of Finite Fields*, Kluwer Acad. Publ., 1993.
3. S. Gao and H. W. Lenstra, Jr., Optimal normal bases, *Designs, Codes and Cryptography* **2** (1992), 315-323.
4. K. Ireland and M. I. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd ed., Springer-Verlag, 1990.
5. N. Koblitz, Elliptic curve cryptosystems, *Math. Comp.* **48** (1987), 203-209.
6. N. Koblitz, CM-curves with good cryptographic properties, *Advances in Cryptology – Crypto '91*, Springer-Verlag, 1992, 279-287.
7. N. Koblitz, *A Course in Number Theory and Cryptography*, 2nd ed., Springer-Verlag, 1994.
8. N. Koblitz, *Algebraic Aspects of Cryptography*, Springer-Verlag, 1998.
9. N. Koblitz, A. Menezes, and S. A. Vanstone, The state of elliptic curve cryptography, to appear in *Designs, Codes and Cryptography*.
10. W. Meier and O. Staffelbach, Efficient multiplication on certain non-supersingular elliptic curves, *Advances in Cryptology – Crypto '92*, Springer-Verlag, 1993, 333-344.
11. A. Menezes, *Elliptic Curve Public Key Cryptosystems*, Kluwer Acad. Publ., 1993.
12. A. Menezes, T. Okamoto, and S. A. Vanstone, Reducing elliptic curve logarithms to logarithms in a finite field, *IEEE Trans. Information Theory* **39** (1993), 1639-1646.

13. A. Menezes and S. A. Vanstone, Elliptic curve cryptosystems and their implementation, *J. Cryptology* **6** (1993), 209-224.
14. V. Miller, Uses of elliptic curves in cryptography, *Advances in Cryptology — Crypto '85*, Springer-Verlag, 1986, 417-426.
15. R. Mullin, I. Onyszchuk, S. A. Vanstone, and R. Wilson, Optimal normal bases in $GF(p^n)$, *Discrete Applied Math.* **22** (1988/89), 149-161.
16. National Institute for Standards and Technology, Digital signature standard, *FIPS Publication 186*, 1993.
17. T. Satoh and K. Araki, Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves, preprint.
18. R. Schroeppel, personal communication, Dec. 2, 1997.
19. R. Schroeppel, H. Orman, S. O'Malley, and O. Spatscheck, Fast key exchange with elliptic curve systems, *Advances in Cryptology — Crypto '95*, Springer-Verlag, 1995, 43-56.
20. I. A. Semaev, Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curve in characteristic p, *Math. Comp.* **67** (1998), 353-356.
21. J. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, 1986.
22. N. Smart, The discrete log problem on elliptic curves of trace 1, preprint.
23. J. Solinas, An improved algorithm for arithmetic on a family of elliptic curves, *Advances in Cryptology - Crypto '97*, Springer-Verlag, 1997, 357-371.
24. E. De Win, A. Bosselaers, S. Vandenberghe, P. De Gersem, and J. Vandewalle, A fast software implementation for arithmetic operations in $GF(2^n)$, *Advances in Cryptology — Asiacrypt '96*, Springer-Verlag, 1996, 65-76.